TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

2€
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

HACKER JOURNAL

n.164
www.hackerjournal.it

CELLTRACK
COME TI TRACCIO IL CELLULARE

INTERNET AL TAPPETO
LA FALLA CHE FA TREMARE IL DNS

SPIATI
dalla stampante
INCUBO O REALTÀ

WEB RADIO
(RI)AGGIRATO IL BLOCCO DI PANDORA

QUATTORD. ANNO 8 - N° 164 - 20 NOVEMBRE/3 DICEMBRE 2008 - € 2,00
WLF PUBLISHING

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Chi è senza peccato scagli il primo DRM

"L'uomo ragionevole si adatta al mondo,
e quello irragionevole si ostina
nel voler adattare il mondo a se stesso.
Pertanto, qualunque progresso
dipende dagli uomini irragionevoli".
George Bernard Shaw (drammaturgo irlandese)

Forse non tutti sanno che proprio gli americani, che oggi tanto si (s)battono per far rispettare il copyright a livello internazionale a colpi di DRM, sono stati i più grandi pirati dell'epoca moderna. All'inizio della loro storia il loro comportamento è stato tale e quale quello di alcune industrie cinesi dei giorni nostri: venivano in Europa a copiare brevetti e prodotti e li replicavano al di là dell'oceano, protetti da lacune legali in termini di diritto internazionale e soprattutto dal fatto che una causa a così grande distanza aveva tempi e costi improponibili.

La stessa industria cinematografica americana si è sviluppata principalmente nella costa pacifica per non pagare i diritti che erano stati registrati a New York. Alcuni piccoli produttori, capeggiati da un certo signor Fox (quello che ha poi fondato la 20th Century Fox) si radunarono in un paesino chiamato Hollywood solo perché era molto distante dall'altra costa. Cosa successe poi di quel piccolo paesino lo sappiamo tutti...

Nella storia l'opera del legislatore ha sempre cercato di seguire quelle che erano le pratiche sociali comuni, pur imponendo una regolamentazione che cercasse di tutelare e ribadire principi condivisi. È chiaro a tutti che non sia possibile una totale libertà di diffusione delle opere dell'ingegno ma è altrettanto chiaro che l'applicazione delle leggi esistenti, così come sono adesso, è assolutamente inadeguata.

Le discussioni animano da tempo gli internauti e i più attenti operatori del mondo IT. Interessanti spunti di riflessione in proposito possono venire dal libro "Elogio della pirateria" di Carlo Gubitosa. L'autore ha deciso di rilasciare l'opera sotto licenza Creative Commons BY-NC-ND 2.0 (cioè "può essere riprodotta e distribuita, con ogni mezzo fisico, meccanico o elettronico, a condizione che la riproduzione del testo avvenga integralmente e senza modifiche, ad uso privato e a fini non commerciali"). Puoi scaricare una versione del libro direttamente dalla pagina dedicata su Wikipedia.

Mi piacerebbe sapere cosa ne pensi e... Buona lettura!

The Guilty



HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.164
20 novembre/3 dicembre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Al via esperimento antipirateria



Per sapere chi è Kevin Bermeister bisogna fare un piccolo passo indietro, all'inizio dell'era del peer to peer, quando i tentativi di creare una rete vasta e stabile di sharer hanno causato il proliferare di programmi p2p in tutte le salse. C'erano quelli complessi e quelli meno complessi, quelli più belli da vedere e quelli inguardabili, e c'era anche Kazaa. Che è stata appunto la creatura di Kevin Bermeister ed è stato uno dei programmi più usati su rete FastTrack quando questa rete era al top per i downloader di tutto il mondo. A suo tempo, proprio a causa di Kazaa, Bermeister si è visto accerchiato dalle major discografiche che nulla desideravano più di togliere di mezzo lui e il suo programma, una vera e propria spina nel fianco. Ma i tempi cambiano

Ora Bermeister è entrato in una nuova società insieme al suo cacciatore, Michael Speck un tempo di Music Industry Piracy Investigations, e insieme stanno mettendo a punto un sistema per scovare e neutralizzare i trasferimenti illegali di materiale protetto da copyright sulle reti peer to peer di tutto il mondo. Questo software si basa anch'esso sugli hash dei file scambiati, proprio come il p2p, ma in questo caso il trasferimento sul server ISP degli utenti viene bloccato e il contenuto modificato in informazioni su come comprare legalmente l'opera che si stava scaricando. Lo scopo è quello dichiarato di voler rimuovere ogni traccia di illegalità dal mondo del peer to peer. Per ora il sistema è in fase di test e presto entrerà in funzione, sempre per un periodo di test della durata massima di un mese e attraverso un ignoto provider americano, per monitorare inizialmente la rete Gnutella. Stando a quanto dichiarato da Speck, nessuna informazione personale sui downloader illegali verrà registrata o usata in alcuna maniera, garantendo il rispetto della privacy. Sta bene, ma qui si sta parlando di un controllo continuativo 24 ore su 24 di tutte le trasmissioni peer to peer mondiali, e in combutta con tutti gli ISP e le case discografiche o cinematografiche esistenti. Altro che Grande Fratello.

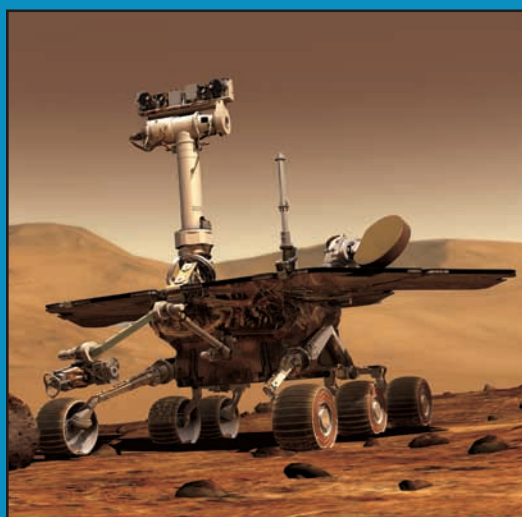
HACKER PER AMORE

Se state pensando di chiedere la mano della vostra ragazza, prendete spunto da Phill, che per la fatidica domanda ha addirittura hackerato Chrono Trigger, il videogame preferito della dolce metà. Ha quindi trasposto se stesso e la loro vita insieme nel gioco, facendole rivivere alcuni momenti del passato, fino a quando, nei panni del personaggio finale del livello, non ha chiesto alla ragazza di sposarlo, mentre nella vita reale si è inginocchiato con tanto di anello di fidanzamento. Senza dubbio una maniera originale...



AL VIA IL NETWORK INTERPLANETARIO

Sulla carta è già una realtà, e si sta passando alla fase di sperimentazione, per cui dovrebbe essere tutto pronto nel corso del 2009. Il papà di questa nuova tecnologia è nientemeno che Vint Cerf, lo stesso il cui lavoro ha dato origine al TCP/IP e a Internet stessa. DTN (Disruption-Tolerant Networking System) sfrutterà ogni veicolo, sonda o satellite lanciato nello spazio da qui in avanti come nodo di inoltro del segnale. In questa maniera tutti i dispositivi locali sulla superficie di un pianeta (come i robottini inviati su Marte) parleranno tra loro con il TCP/IP, mentre il nodo principale marziano invierà i dati verso la terra instradandoli verso il nodo più vicino usando il nuovo standard DTN. Se tutto va bene, già dal 2010 l'Internet interplanetaria sarà una realtà operativa.



MP3 VIA RADIO

Un nuovo chip Bluetooth di Broadcom, denominato BCM2049, porterà presto l'ascolto di musica in Mp3 e formati simili a un nuovo livello. Basterà infatti disporre di un ricevitore FM stereo nei pressi e di un dispositivo basato sul nuovo chip per trasmettere l'audio dall'uno all'altro via etere. Una cosa che in realtà già si può fare, ma questo nuovo chip aggiunge un po' di sale alla pietanza: dispone di un ricevitore FM in grado di individuare le frequenze più libere per usarle per la trasmissione, quindi non avremo più problemi di disturbi o di sovrapposizione di segnale, specialmente mentre ci spostiamo in auto. In più grazie alla tecnologia Bluetooth un dispositivo basato su questo chip potrà essere usato con normali cuffie o auricolari senza fili già in nostro possesso. Dobbiamo solo aspettare che i produttori lo integrino presto nei propri prodotti, ma già immaginiamo i vantaggi di un cellulare con questo chip.





HOT NEWS

OSCURATO IL MINISTRO... CONTESTATO IL MINISTRO



In pieno marasma a causa della riforma della scuola ideata dal ministro Gelmini, ognuno dice la propria e si schiera da una parte o dall'altra. Accade così che un consigliere regionale della Lombardia, Carlo Saffioti, crei addirittura un sito per appoggiare e sostenere la Gelmini e la sua riforma (www.forzagelmini.com), e accade anche che qualcuno pensi bene di buttarlo giù. È successo alla fine di ottobre: gli hacker con il più classico dei DDoS hanno impallato il server su cui gira il sito, che è riapparso online poche ore dopo ma in una versione non aggiornata (i messaggi presenti risalivano ad alcuni giorni prima). Intanto l'iter della legge è proseguito, con l'approvazione del Senato.

GIUSTIZIA CONTORTA

Può capitare, navigando nella rete locale o su Internet, di accedere per sbaglio o meno ad aree e a dati per cui non abbiamo diritto di accesso. Può capitare che questo avvenga a causa di una falla della sicurezza nel sistema, che magari non stavamo nemmeno cercando di attaccare. Può anche capitare che, certi di fare del bene, si segnali la cosa all'autorità competente e che, in tutta risposta, si finisca al fresco per essersi intrufolati nel sistema. È quello che è accaduto a uno studente americano di 15 anni: dopo aver avuto accesso a un'area riservata contenente dati sensibili semplicemente inserendo la propria password durante le ore di lezione, ha segnalato la cosa al preside, che però l'ha denunciato alle forze dell'ordine come cracker, facendolo finire agli arresti. Brutto esempio di ignoranza informatica. Quella del preside.



Wii BLINDATA?

Pochi giorni fa si è reso disponibile un aggiornamento del firmware della popolare console di Nintendo che, tra le altre cose, implementa un nuovo sistema di protezione contro gli hacker che intendono installare Homebrew Browser. Durato due giorni: anche questo blocco è stato spazzato via dagli appassionati e ancora una volta è possibile scaricare e installare software alternativo sulla Wii e usare schede SDHC, inizialmente non implementate dalla casa nipponica. Pare però che in futuro Nintendo intenda essere meno flessibile e imporre blocchi più definitivi. Per la maggior parte chi cracca la Wii lo fa per usare emulatori e giocare con vecchi giochi per NES, SNES o altre console datate, e Nintendo stessa ha riesumato quei vecchi titoli per guadagnare ancora un po' con essi proprio attraverso Virtual Console.



Internet Service Providers in rivolta

Lo fanno per amor di legge e perché sono obbligati, ma non ne sono contenti e protestano con forza, tanto da presentare richiesta di intervento alla magistratura. Parliamo degli ISP italiani, costretti dalle forze dell'ordine a oscurare di fatto due siti Web che vendono sigarette illegalmente (in Italia, per via delle leggi sul monopolio di stato) filtrandoli fuori dalle connessioni del Bel Paese. Non tanto perché non siano d'accordo con l'illegalità della vendita di sigarette, ma per il fatto che questo obbligo costituisce un pericoloso precedente (al pari con la vicenda The Pirate Bay) che li costringerebbe in futuro a essere sempre più sceriffi della rete e sempre meno fornitori di servizi. Restiamo in attesa di sviluppi.



FACEBOOK SULLA MAGLIETTA

Una nuova frontiera per il social networking o, come qualcuno l'ha definita, una nuova tecnica per tacchinare le ragazze (o per accalappiare ragazzi). Non serve più nemmeno attaccare bottone, non subito almeno: faccio una foto a un particolare disegno sulla tua maglietta e posso accedere al tuo profilo su Facebook direttamente dal cellulare.
Perché quel disegno è in realtà un codice a barre bidimensionale, in cui è codificato il tuo indirizzo su Facebook (o quello del tuo sito, o la tua e-mail, o un altro mezzo per contattarti) e l'applicazione che ho sul mio telefonino è in grado di interpretarlo e di mettermi in comunicazione con te. Grazie a W-41, azienda olandese che ha ideato e commercializzato il sistema.



WIKIPEDIA SU DVD

Di recente è stata resa disponibile una versione di Wikipedia dedicata ai ragazzi delle scuole, liberamente scaricabile via torrent e masterizzabile su DVD. Contiene circa 5500 articoli, pari più o meno al contenuto di una tradizionale enciclopedia da 20 volumi, accuratamente selezionati e adattati perché possano essere fruibili dal pubblico dei più piccoli: ogni riferimento a violenza, pornografia e ad argomenti non adatti è stato rimosso. Può anche essere consultata online all'indirizzo http://schools-wikipedia.org/ (per ora disponibile solamente in lingua inglese dato che il progetto nasce per le scuole del Regno Unito, ma speriamo che presto possa essere trasposta anche in italiano).
Una comodità che speriamo possa essere estesa anche ad altri settori di interesse, per esempio permettendo agli utenti di compiere una propria selezione degli articoli e di scaricare gli argomenti scelti per masterizzarli e consultarli anche offline.



ASL BUCATE

L'Osservatorio nazionale per la sicurezza informatica ha condotto un'indagine sullo stato di salute delle nostre ASL, dove quotidianamente circolano dati personali e sensibili di migliaia di persone. Il risultato: il 60% delle 50 ASL prese a campione aveva seri problemi di sicurezza ed erano facilmente attaccabili, mentre l'85% non ha abbastanza soldi per far fronte al problema. È un attimo, se il vostro vicino vuole curiosare sul vostro stato di salute o nella vostra cartella clinica, non ha bisogno di appostarsi alla finestra, gli basta andare su Internet.



WINDOWS AZURE

È già disponibile in prova per gli sviluppatori una nuova versione di Windows. Non si tratta di Windows 7 né di un sistema operativo tradizionale, dedicato al nostro PC di casa, ma piuttosto di una piattaforma di sviluppo basata sul Web che darà ai programmatori la possibilità di scrivere applicazioni per il cloud computing, cioè applicazioni e servizi distribuiti sul Web e che l'utente finale può usare anche se non diretta-

HOT NEWS

LAVANDERIE CONTRO IL TERRORISMO

La notizia trapela solo ora ma è da tempo che i servizi segreti britannici hanno adottato una strategia inconsueta per scovare e fermare in tempo i terroristi dell'IRA.
Niente 007 appostati agli angoli delle strade occupati in pedinamenti, ma lavanderie automatiche negli stessi angoli che, con uno speciale scanner costruito per rilevare tracce di esplosivi, annusa gli abiti prima che finiscano nelle lavatrici. In questo modo pare che siano stati individuati diversi terroristi e salvate moltissime vite sequestrando esplosivi e ordigni di vario tipo. Pare che anche gli USA vogliano adottare una strategia simile nelle loro sfortunate campagne in Medio Oriente...



VOGLIONO SOLDI ANCHE DAI PROVIDER



Per fortuna la notizia è stata smentita, ma per qualche mez-z'ora ci ha fatto temere il peggio, dato che ormai non sanno più dove attaccarsi e dove spillare quattrini: la SIAE, secondo le voci, pretenderebbe una legge che obblighi i provider che offrono connessioni a banda larga a pagare un contributo economico per rimpinguare le proprie casse, con la scusa che questo tipo di connessione invoglia gli utenti a scaricare liberamente materiale protetto dai diritti d'autore. Chi si ricorda quando ha preteso il balzello anche sulle suonerie dei cellulari? Certo è che, se una richiesta simile venisse assecondata, vedremo tutti un bell'aumento sulle tariffe degli abbonamenti Internet, a dispetto di tutte le pressioni per la libera concorrenza dei prezzi voluta dalle associazioni dei consumatori. Perché qualcuno, quei soldi, dovrà pur sborsarli...

YAHOO VERSO IL SOCIAL

Ancora si vivono gli strascichi della tormentata vicenda Microsoft, e Google ormai è in situazione predominante per quanto riguarda l'advertising sul Web, ma Yahoo non molla e decide di cambiare strategia. Sostanziale, perché lo scostamento è sempre più verso l'open source; di concetto, perché forte della presenza (ma non confermata) di più di 500 milioni di iscritti, l'intenzione è quella di dare un accento in più al social networking. Per il momento Yahoo ha reso disponibili liberamente librerie PHP e Flash per gli sviluppatori contenenti elementi e strumenti adatti per creare piattaforme social networking alla stessa stregua di Facebook; vedremo come questa svolta verrà recepita dal pubblico.

mente disponibili sul proprio PC. Anche se la versione commerciale non vedrà la luce probabilmente fino al 2010, gli sviluppatori potranno iniziare a prendere confidenza con il mezzo, che si integra comodamente con Visual Studio.



OPERA PATCHATO

Sono passati pochi giorni dall'uscita della nuova release di Opera ed è già tempo di patch.
È stata scoperta infatti una grave falla di sicurezza che permetterebbe a un sito malintenzionato di eseguire codice sul computer di chi lo visita.
Questa falla è stata scoperta da Roberto Suggi Liverani, Aviv Raff e Stefano di Paola. Si tratta di una debolezza di tipo stored cross site scripting, dello stesso tipo quindi di quella corretta dall'ultima patch per il programma.
Aviv Raff lo ha dimostrato creando sul proprio sito una pagina in grado di far eseguire al computer "vittima" la calcolatrice di Windows in automatico.

Scripta MANENT



La stampante laser a colori appena comprata potrebbe non esserci amica. Ecco come ci frega

Una leggenda metropolitana informatica narra come Bill Gates sia riuscito a scrivere MS-DOS nel suo garage aiutandosi con codici sorgenti rubati ai programmatori di altre aziende. La cosa buffa è come si è procurato quei sorgenti: andandoli a ripescare dai rifiuti. Vero o falso che sia, il dubbio è come possa aver riconosciuto con precisione le stampe che riguardavano i sorgenti, in mezzo alle tonnellate di carta che ogni giorno un'azienda può produrre (soprattutto a quei tempi).
Oggi non siamo molto lontani dalla leggenda, anzi chi volesse ottenere informazioni a partire da una stampa può farlo quasi senza sforzo, a patto che sappia dove guardare.

:: Tutta colpa dei falsari

La notizia in realtà non è nuovissima, ma rimane sempre di attualità, perché gli studi sulla faccenda sono ancora in corso.
Tutto nasce dall'enorme progresso tecnologico in ambito informatico del periodo che stiamo vivendo: fino a metà degli anni '80 le stampanti erano a margherita (cioè stampavano mediante un disco con caratteri fissi, detto appunto margherita: come le macchine da scrivere) o al massimo a matrice di punti (dove i caratteri erano formati dagli aghi di una testina che battevano sul retro del nastro inchiostrato per spingerlo sulla carta), ora chiunque con poche centinaia di euro può portarsi a casa una stampante laser a colori in grado di produrre stampe talmente definite che sembrano uscite dalle macchine di una tipografia.
Ed ecco il pericolo: stampe così definite potrebbero permettere di replicare materiale originale, anche se protetto da filigrane o accorgimenti simili, in maniera talmente precisa da non riuscire più a distinguerlo dalla copia.
La manna per i falsari di tutto il mondo, chi non vorrebbe stamparsi un paio di centoni prima di uscire con la ragazza?

:: E allora ti marchio

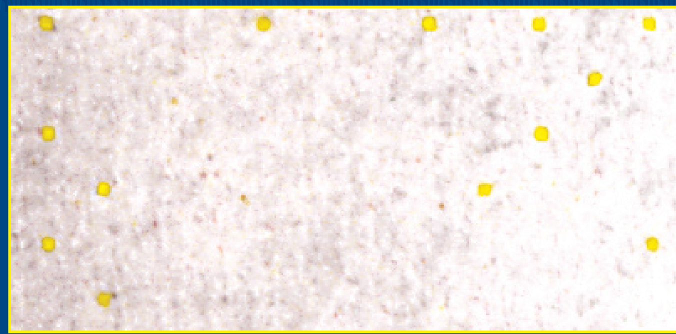
Nel 2005 la Electronic Frontier Foundation è riuscita a craccare un codice stampato di nascosto dalle stampanti laser prodotte dalla Xerox su ogni stampa. Si tratta di microscopici punti di colore giallo, praticamente invisibili a occhio nudo sul bianco della carta, disposti in maniera diversa in base alla data e all'ora di stampa e al numero seriale della stampante che l'ha prodotta. Non è difficile, ora che si sa della loro esistenza, scovare questi punti nei fogli prodotti da stampanti incriminate, ma fino al lavoro di EFF nulla si sapeva di cosa volessero dire, si pensava anzi che potessero essere sbavature di colore.

:: A caccia di punti

Se non abbiamo a disposizione un microscopio abbastanza potente,



Sono quasi invisibili, ma qui ci sono i punti gialli.



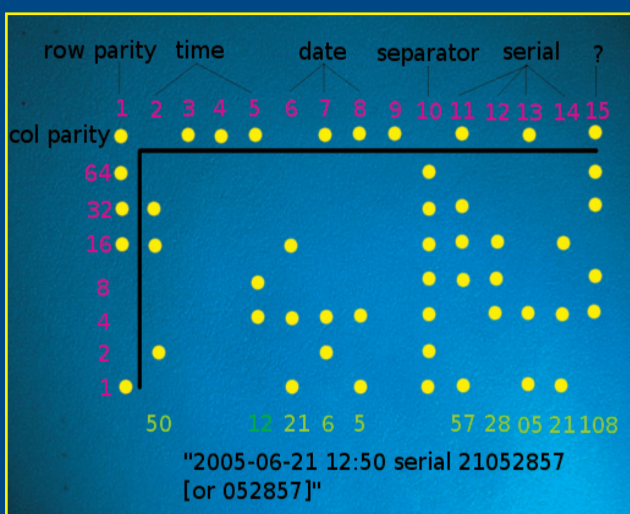
Eccoli visti al microscopio.

possiamo scovare i famigerati punti gialli usando qualche piccolo trucco. Il più semplice richiede una fonte di luce blu (molti portachiavi con LED oggi illuminano di blu, non dovrebbe essere difficile trovarne uno): illuminando di sbieco con la luce blu un foglio proveniente da una stampante laser, infatti, questi punti diventano visibili come piccole macchie scure disposte in maniera abbastanza regolare lungo il margine della. Comunque bisogna avere un occhio di falco per riuscire a vederli, dato che sono davvero piccolissimi.
Possiamo quindi farci aiutare dalla tecnologia: se abbiamo a disposizione uno scanner ad alta risoluzione (meglio intorno ai 4800 dpi per poter ingrandire adeguatamente l'immagine mantenendo un po' di nitidezza), possiamo riprendere la stampa in formato elettronico e passarla poi in un programma di grafica.
Qui, separando i tre canali RGB e prendendo in esame solamente il canale blu e ingrandendo, dovrebbero risultare visibili come punti scuri.

:: Leggiamoci chiaro

EFF è riuscita a individuare con precisione il significato di alcuni di questi punti gialli, secondo lo schema che andiamo ora a decifrare. I punti sono disposti sotto forma di matrice, un rettangolo di 15 byte da 8 bit l'uno, dei quali se ne considerano solo 7 essendo l'ultimo il bit di parità.
Riportandoli su un grafico, avremo sull'asse X i 15 byte, sull'asse Y i singoli bit di ogni byte, in questo modo è possibile leggere facilmente il contenuto del codice, una volta che se ne conosce il significato. Lo schema va letto da destra a sinistra e troviamo, nell'ordine:

- **byte 15**: sconosciuto, spesso a 0, ma costante per ogni stampante; potrebbe avere a che fare col modello o la configurazione della stessa;
- **byte da 14 a 11**: il numero di serie della stampante, unico e costante per ogni stampante;
- **byte 10**: separatore, tutti i suoi bit sono sempre settati e pare che non contenga informazioni;
- **byte 9**: non usato;
- **byte 8**: anno senza il secolo (quindi 2008 sarà rappresentato da un byte di valore 8);
- **byte 7**: mese in cui è stata stampata la pagina;
- **byte 6**: giorno in cui è stata stampata la pagina;
- **byte 5**: ora della stampa (potrebbe essere l'ora UTC ma anche un'ora mal impostata nella stampante);
- **byte 4 e 3**: non usati;
- **byte 2**: minuto della stampa;
- **byte 1**: contiene i bit di parità di riga.



La tabella di decodifica scovata da EFF.

Se nella nostra stampante troviamo questi punti gialli, quindi, sappiamo per certo che chi recupera una nostra stampa potrebbe essere in grado di risalire all'autore attraverso il numero seriale indicato.
Se li scoviamo possiamo decodificarne il significato con un semplice script messo a disposizione da EFF all'indirizzo http://w2.eff.org/Privacy/printers/docucolor/.
Chiaro che la tracciabilità delle nostre stampe dipende anche da altri fattori: per esempio, bisogna per forza avere una documentazione, come una fattura o una bolla di qualche tipo, per sapere che quel preciso modello di stampante è in nostro possesso, quindi la situazione è molto più pericolosa per una grande azienda piuttosto che per il privato cittadino, ma non si sa mai.
Comunque, all'indirizzo http://www.eff.org/Privacy/printers/list.php è presente un elenco di stampanti testate da EFF con il relativo responso.
Non trovare i punti gialli non vuol dire automaticamente essere al sicuro: all'indirizzo http://cobweb.ecn.purdue.edu/~prints/ troviamo (in inglese) informazioni su altre tecniche definite "printer forensics" che permettono di rintracciare una stampante (e quindi il proprietario) a partire dalla stampa. Un buon distruggi-documenti di quelli da ufficio è sempre un ottimo investimento.

Oltre l'apparenza

Scopriamo i segreti della struttura dei file che stanno alla base della steganografia



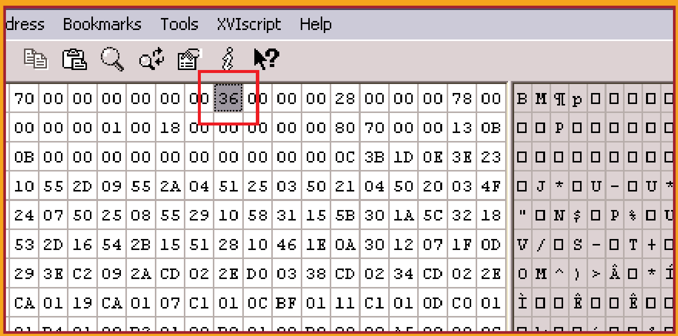
La crittografia è un ottimo sistema per nascondere informazioni che devono rimanere segrete, ma ha un problema di base: le informazioni sono fisicamente visibili anche se incomprensibili finché non vengono decrittate. Per questo motivo è nata la steganografia, una tecnica che permette lo scambio di informazioni in cui lo scambio stesso, e non solo le informazioni passate, rimane segreto.

Siamo hacker o caporali?

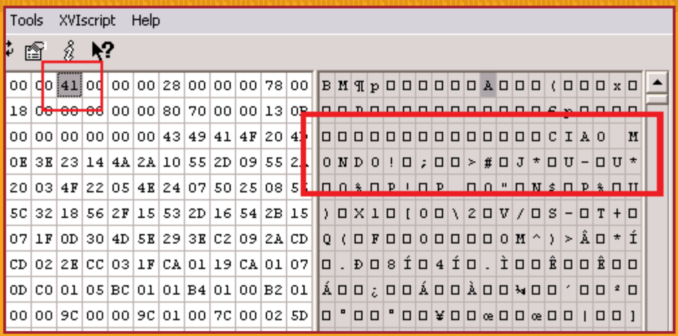
Non vogliamo trattare qui la steganografia o il watermarking in sé, sono cose già trite e ritrite che tutti ormai conosciamo a menadito.
Più o meno. C'è una piccola differenza di sostanza tra il conoscere l'intima natura di una cosa e semplicemente usarla per quello che è. Tutti sono capaci di fare un giro sul Web, scaricare il primo programma per la steganografia che pare adeguato, usarlo per nascondere i dati in un'immagine e spedire il tutto al destinatario. Anche il vero hacker lo fa, ma in una maniera del tutto differente: l'hacker sa come funzionano le cose e sa piegarle a proprio vantaggio, non si limita a usare il "4 file in padella" dell'information hiding ma si prepara da solo un pranzetto luculliano. Il vantaggio è evidente: anche i criceti sanno che la palette di una bitmap viene usata per nascondere la chiave di decodifica di un'immagine o di un testo nascosti, ma nessuno potrà mai sapere come siamo riusciti noi a nascondere un messaggio, perché noi la chiave non la nascondiamo nella palette, ma riusciremo a escogitare un sistema nuovo e sconosciuto, con buone probabilità che non sia mai stato usato prima. È così che il vero hacker crea i propri ferri del mestiere. Scopriamo perché questo è possibile.

Apriamo la scatola

Prendiamo in esame la classica immagine che fa da contenitore per il messaggio nascosto, una semplice bitmap di Windows che è un formato semplice da leggere anche ad occhio (intendo proprio guardandone la struttura del file, un po' come Cypher guardando il codice di Matrix vedeva bionde, brune, belle gambe e così via); il concetto lo potremo ap-



L'header di un'immagine bitmap in un editor esadecimale. Il byte evidenziato nel riquadro rosso indica l'offset dei dati dell'immagine a partire dall'inizio del file.



Stesso header ma con un messaggio nascosto. Il byte di offset manda i programmi di visualizzazione all'inizio dei dati, lasciando spazio per salutare il mondo.

plicare a qualsiasi formato grafico e, estendendone l'uso, a qualsiasi tipo di file.
La prima cosa da fare è studiare bene il formato del file che intendiamo usare come vettore per i nostri messaggi segreti. Solamente così potremo trovare le sue debolezze e sfruttarle per crearci spazio e inserire un messaggio nascosto usando un sistema personalizzato. I blocchi di dati che compongono un'immagine bitmap sono quattro:

1) **BMFileHeader**: contiene le informazioni sul file;
2) **BMInfoHeader**: contiene le informazioni che riguardano l'immagine contenuta nel file;
3) **BMColorTable**: la palette dei colori, quando necessaria;
4) **BMImageData**: i dati dell'immagine, cioè i pixel che la compongono.

Il blocco **BMFileHeader** contiene un dato importantissimo. I primi due byte (WORD) sono le lettere BM, che indicano il formato del file. I quattro byte successivi (DWORD) riportano le dimensioni dell'immagine. Seguono poi due gruppi di due byte ciascuno (WORD, WORD) riservati per sviluppi futuri e normalmente sempre a zero. L'ultimo gruppo di due byte (WORD) indica il punto di inizio dei dati dell'immagine a partire dall'inizio del file: **è questo il dato che ci interessa**.
Infatti, se aumentiamo questo valore, avremo creato automaticamente spazio per includere un messaggio nascosto. Per esempio, in una bitmap a 16 milioni di colori questo valore è pari a 0x3600 (54 in decimale), significa che se portiamo tale valore a 0x4100 (che equivale a 65) potremo inserire le parole CIAO MONDO! tra la fine degli header e l'inizio dei dati immagine, senza che l'immagine stessa venga compromessa.
È un sistema troppo semplice: basta aprire l'immagine con un editor esadecimale o anche nel Blocco note per mettere in bella mostra il nostro messaggio. Però è un inizio.

Scaviamo più a fondo

Se conosciamo bene la "scatola" che stiamo usando, possiamo anche spingerci oltre, ma non basterà più un editor esadecimale, avremo bisogno di scrivere un programma ad hoc. Possiamo per esempio codificare il messaggio nell'immagine senza aumentare le dimensioni del file, principio alla base delle più diffuse tecniche di steganografia. Con un'immagine a 256 colori un po' disturbata, o con ampie aree di tonalità molto simili, possiamo riservare 36 colori della palette (26 lettere e 10 cifre) per la codifica del messaggio, usando gli altri 220 per l'immagine. Questi colori possono essere consecutivi o no, e il messaggio può essere nascosto riga per riga, dall'alto verso il basso o a spirale.
Potremmo anche usare un'immagine a 16 milioni di colori con una forte predominanza di un colore primario (ad esempio un papavero in un campo). In questo caso i pixel sono rappresentati da terne di valori RGB e con predominanza per esempio di rosso avremo un valore nel byte R e probabilmente zero negli altri due byte.
Se nel nostro programma decidiamo che la codifica di un carattere è il suo codice ASCII normalizzato a zero (cioè il valore più basso è codificato con zero, il carattere successivo con 1 e così via) potremo inserire i valori corrispondenti ai caratteri in questi byte dell'immagine senza che questo risulti visibile a occhio nudo.



In un'immagine così possiamo inserire quello che vogliamo, ma dobbiamo farlo con originalità o sarà facile venire scoperti.

Privateer

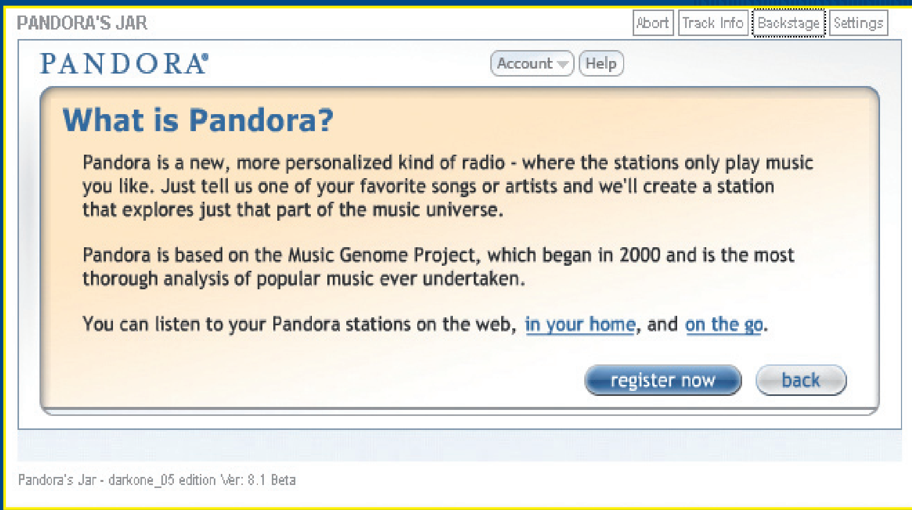
PANDORA WEB RADIO: IL GENOMA MUSICALE

Aggirato il blocco che non consente agli utenti al di fuori degli USA di accedere al sito

Nel gennaio del 2000 a un gruppo di musicisti e amanti delle nuove tecnologie venne in mente di realizzare l'analisi più completa e approfondita mai svolta sulla musica. Quest'analisi si basava sulla comparazione di centinaia, di canzoni e identificò, tramite un complesso algoritmo, quelli che vengono chiamati attributi o "geni" musicali al pari del DNA (da cui il nome del progetto di Genoma Musicale). L'obiettivo era quello di "catturare l'essenza della musica fino alle sue particelle primarie". La magia di una musica è fatta di armonia, melodia, ritmo, e, ovviamente, dell'interpretazione, ovvero dall'unione di questi "geni" e per identificarli, fin dall'inizio del progetto sono stati ascoltati i brani di circa diecimila artisti, variando la scelta tra quelli più famosi a quelli più sconosciuti. Quest'attività è continuata e prosegue quotidianamente con il feedback di studi di registrazione, club e garage sparsi in tutto il mondo.

Pandora (www.pandora.com). è il software online che utilizza questo algoritmo e che si interfaccia con il





La schermata iniziale di Pandora da cui è possibile registrarsi al servizio.

database musicale ,in continua crescita, a disposizione del progetto permettendo di realizzare nel contempo delle radio virtuali capaci di proporre brani musicali sintonizzati con estrema precisione sul gusto dell'utilizzatore. È sufficiente inserire il nome di un artista, il titolo di una canzone o un genere musicale che ci piacciono per trovare centinaia, se non migliaia, di brani compatibili con i nostri gusti. Se inseriamo artisti o canzoni famose solitamente queste vengono offerte come prima scelta, successivamente vengono proposte all'infinito canzoni e brani "simili", ovvero che si avvicinano al genere e al ritmo del brano di partenza. Infatti fin dalla selezione del primo brano vengono identificati i geni musicali che sono alla base del nostro gradimento e su quella base l'algoritmo continua a selezionare e riprodurre nuovi brani.
È possibile aiutare l'algoritmo fornendo il proprio feedback sul gradimento positivo o ne gativo delle proposte del sito, ma anche senza questo il software è in grado di stupire! Provare per credere.

:: La censura americana

Per rendersi conto di quanto è semplice utilizzare Pandora, basta, o per meglio dire basterebbe, andare sul sito ufficiale e provare a lanciare qualche richiesta.
Purtroppo nel Marzo 2007 la Riaa (la SIAE statunitense) ha triplicato le royalties sugli ascolti online e ha di fatto obbligato Pandora (e le altre radio virtuali) a prendere accordi con tutte le associazioni omologhe in ogni stato ove avesse potuto trasmettere le sue radio virtuali. Richiesta peraltro inattuabile data la globalità di Internet. Il presidente di Pandora, Tim Westergren, organizzò una petizione online per richiedere la non attuazione di queste nuove misure auspicando la nascita di una regolamentazione internazionale delle royalties, ma finora nulla si è mosso.
Di conseguenza Pandora è stata di fatto obbligata a bloccare gli accessi provenienti al di fuori degli Stati Uniti; un blocco davvero inaccettabile se pensiamo che il servizio è nato proprio per mettere in contatto musicisti e ascoltatori di tutto il mondo. Per l'Italia il blocco è attivo da maggio 2007. Ma è stato aggirato.

:: Hack it!

Applicando un filtro basato unicamente sull'indirizzo IP dell'internauta che va sul sito di Pandora è abbastanza semplice superare il blocco perché tramite un **software proxy è possibile far apparire la propria connessione come proveniente dagli Stati Uniti invece che dall'Italia**. Le soluzioni trovate per accedere a Pandora sono diverse,ne presentiamo una delle più utilizzate.
Prima di tutto è necessario scaricare e installare l'ultima versione di Vidalia Bundle (al momento in cui scrivo la 0.2.0.31-0.1.9) per il proprio sistema operativo dal sito ufficiale www.Vidalia-project.net; il bundle include Vidalia e Privoxy, entrambi sono software opensource; una volta installato, dai menu si seleziona Vidalia Bundle → Tor → Torrc.
Quindi, utilizzando il Blocco note di Windows, si inseriscono in fondo al file le seguenti due righe (senza apici) e si aggiunge un a capo dopo la seconda (ricordatevi di salvare prima di chiudere Blocco note): si crea un semplice file di testo inserendo esattamente queste righe e lo si salva come C:\tor.pac.

```
"StrictExitNodes 1"
"exitnodes desync,whistlersmother,lefkada,bettyboop,croeso,TorLuwakOrg,nixnix,inap1,redpineapple,cronic,sasquatch,slowturtle2"
```

```
function FindProxyForURL(url, host)
{
if (shExpMatch(host, "www.pandora.com")) return "SOCKS 127.0.0.1:9050";
// All other requests don't pass proxy
return "DIRECT";
}
```

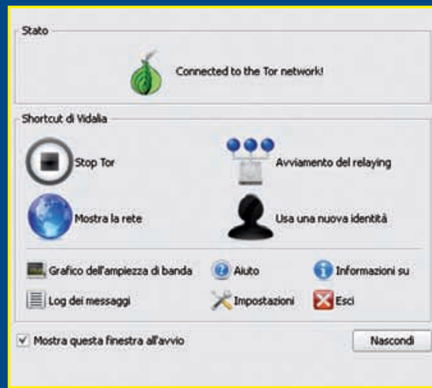
Ogni browser che si vuole usare per accedere a Pandora va configurato in modo che usi il file tor.pac:

- **per Internet Explorer**: Opzioni Internet → Connessioni → Impostazioni LAN → spuntare Utilizza script di configurazione automatica e inserire nel box "file://C:\tor.pac"
- **per Firefox**: Strumenti → Opzioni → Rete → Impostazioni → spuntare "Configurazione automatica dei proxy (URL)" e inserire "file:///C:/tor.pac"

A questo punto si avvia, o si riavvia se già lanciato, Vidalia (Start → Programmi → Vidalia Bundle → Vidalia) e si aspetta che indichi che il collegamento al network TOR è attivo (l'icona nel tray diventa verde).
È importante accertarsi che sia in funzione anche Privoxy (è visibile una P simile al segnale di parcheggio nel tray), altrimenti lo si lancia (Start → Programmi → Vidalia Bundle → Privoxy → Privoxy).
Infine si rilancia il browser e si va all'indirizzo www.pandora.com (è importante avere installato Flash 8 o superiore, si trova sul sito di Adobe).
Da questo momento è possibile ascoltare Pandora come se si accedesse dagli Stati Uniti (la navigazione di tutti gli altri siti non è influenzata perché i file di configurazione riguardano solo le richieste verso www.pandora.com), senza commettere alcun reato in quanto, come sappiamo, nessuno può vietarci di adottare misure atte a proteggere la privacy della nostra navigazione.
Dopo un po' il programma chiederà di effettuare la registrazione, sarà sufficiente inserire un CAP degli Stati Uniti (ZIP code) che viene richiesto a fini statistici.
Se ne può scegliere uno a caso da www.zip-area.com e il gioco è fatto!

:: Gratis 100%? No, ma va bene così

Pandora è un servizio di ascolto gratuito che non prevede alcun canone; la registrazione (gratuita) è necessaria al solo scopo di permette all'algoritmo di costruire un profilo tarato esattamente sui gusti dell'utente).
Ma Pandora è anche uno store online dove con pochi clic è possibile acquistare brani di artisti che con molta probabilità non avremmo mai conosciuto tramite i classici canali di vendita dominati da politiche commerciali o mode del momento.
Ed è qui la fonte di reddito e allo stesso tempo il plus di Pandora: indovinare con la massima precisione i gusti dell'ascoltatore per proporgli il prodotto più adatto e originale.
E se vi chiedete perché attaccare un



Il pannello principale di Vidalia per l'accesso alla rete TOR.

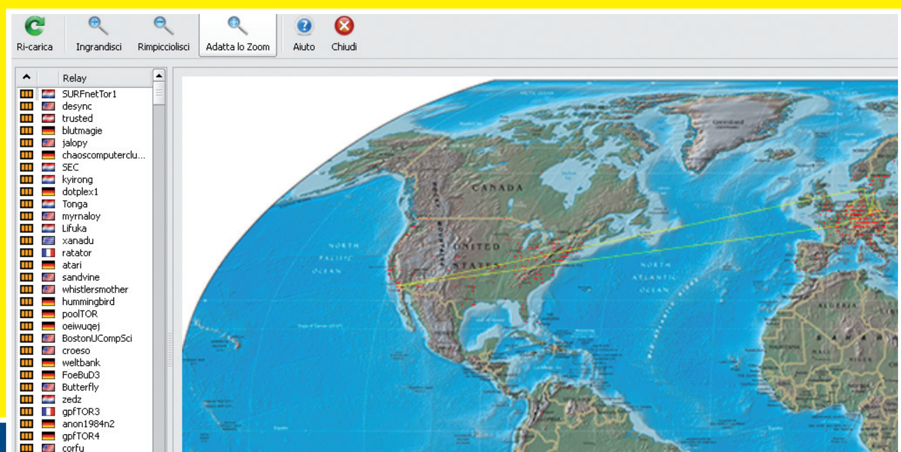
modello di business innovativo e stimolante la risposta è presto detta: è evidente che le major che muovono gli interessi della Riaa, non siano assolutamente al passo con le tecnologie ma soprattutto non amano che la musica possa circolare liberamente al di fuori dei canali distributivi così ben controlati. La battaglia tra business e futuro è sempre aperta, nel campo della musica come in quello dei software o dei brevetti genetici, noi vigiliamo e cerchiamo di far sentire la nostra voce.

:: Crack it!

Pandora funziona in modalità streaming, ossia ci invia online il brano che stiamo ascoltando.

CIPOLLE PER DIVENTARE ANONIMI

La rete TOR (The Onion Ring) è un sistema di router sparsi in tutto il mondo e gestiti da volontari che permette il traffico anonimo sul Web.
In pratica, rende impossibile tracciare e analizzare i nostri movimenti sulla Rete, garantendo il nostro anonimato. In più il traffico è completamente cifrato, praticamente impossibile da intercettare se non nel tratto finale, dove la trasmissione è in chiaro. Per usare la rete TOR bisogna installare l'apposito software prelevato da www.torproject.org.

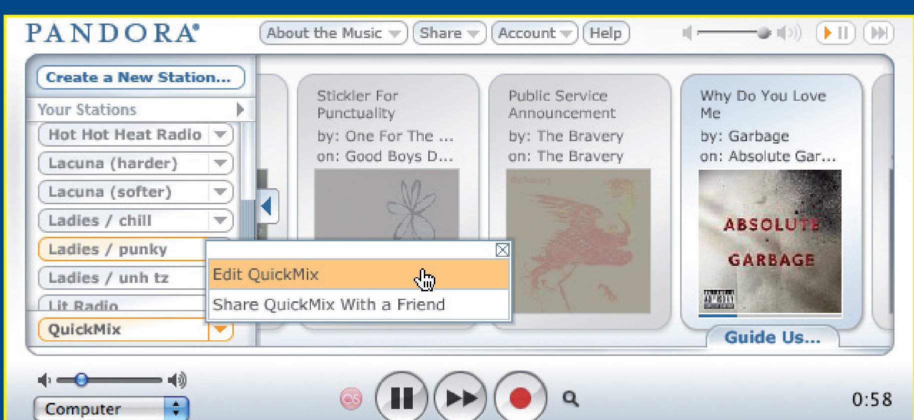


Ma ormai le connessioni a banda larga permettono di ricevere l'intera canzone, e di fatto averla nella cache del programma, molto prima che si sia finito di ascoltarla. Anche se offuscato e reso irriconoscibile il file in formato MP3, in play dopo una manciata di secondi, è lì sull'hard disk.
Facile capire quindi che non è un'operazione complicata scovare questo file e salvarlo in chiaro sul nostro PC. Ma è bene tenere presente che si tratta di un'operazione estremamente illegale e moralmente discutibile: rubare la musica di artisti emergenti, ma non farebbe differenza se fossero ricchi e affermati, ha lo stesso effetto delle peggiori azioni censorie delle varie Riaa di tutto il mondo.
Tuttavia non tutti hanno sani principi morali, ed è bastato poco a un gruppo di cracker per creare Pandora's Jar, un'applicazione Java (occorre aver installata l'ultima versione del Java Runtime Environment, scaricabile eventualmente da java.sun.com) ovviamente illegale in grado di salvare e organizzare per bene i brani ascoltati su Pandora, con tanto di tag Id3 compilati accedendo a CDDB.
Tutte le informazioni su come scaricare, installare e configurare il programma si trovano sul sito hack5.org, ma non è dato sapere fino a quando saranno disponibili (è sempre possibile una chiusura forzata da parte delle forze dell'ordine). L'applicazione permette addirittura di aggiungere i brani anche alla libreria di iTunes, così come pemette di agganciarsi al database di last.fm e informare il social network su quale brano stiamo ascoltando. Il procedimento è simile all'ascolto diretto, il programma accede a Pandora via proxy americano. Nelle impostazioni si può scegliere se attivare il Cruise Control, una funzione che salva automaticamente tutti i brani ascoltati senza alcun intervento. In caso contrario per salvare il brano in ascolto si deve fare clic sul pulsante Grab This Track presente nell'interfaccia. Il vaso di Pandora è stato aperto, non rubiamo i cocci!

NoeXKuzE



La schermata di Pandora's Jar.



La schermata di Pandora durante l'ascolto.

Soluzione di scorta

Dato che è sempre incerta la tenuta della rete TOR (che è legale, ma che è anche in grado di filtrare il traffico indesiderato e potrebbe bloccare l'accesso a Pandora) e che comunque la pratica di salvare i file Mp3 in ascolto non è legale per niente, abbiamo un'altra soluzione che per lo meno ci permette di ascoltare i brani, senza salvarli e al costo di qualche banner pubblicitario. Si tratta di creare un collegamento VPN con un server americano, che non solo renderà la navigazione anonima, ma permetterà di accedere a Pandora senza dover configurare alcunché. Basta scaricare Hotspot Shield, un'applicazione di Anchorfree (anchorfree.com) che dirotta il nostro traffico Internet sul proprio server posto in America. Da lì è possibile ascoltare la nostra musica preferita senza le limitazioni territoriali di Pandora.
Ci sono comunque delle limitazioni: a parte il banner pubblicitario che può non piacere a tutti, si tratta di una VPN con limiti di banda a 600k in download e 280 in upload; sono disponibili fino a 3 GB al mese di banda, oltre bisogna pagare (non va bene quindi se si intende usare il mulo) e giunti al limite si viene disconnessi per uso eccessivo della banda.
Inoltre, l'uso del programma è vincolato al rispetto delle condizioni, che vietano comportamenti illegali (come scaricare a sbafo o tentare attacchi hacking). Ricordiamoci che il server è fisicamente negli USA e che è un attimo vedere i propri log nelle mani dell'FBI...

Il perché dei noiosi CAPTCHA



A cosa servono i Captcha e perché siamo costretti a incontrarli così spesso

Sono brutti e pure fastidiosi. Sono quelle classiche cose che non vorremmo mai dover fare, eppure spuntano come funghi durante la nostra navigazione. Sono le maschere in cui dobbiamo digitare, con assoluta precisione, quelle lettere e numeri quasi indecifrabili che appaiono lì vicino nella pagina. Ma perché mai i siti ci chiedono di compiere quest'azione ben pochi se lo chiedono.

L'esistenza dei Captcha è legata alla necessità di difendersi da quelle persone che usano Internet solo per il loro profitto personale. Parliamo, ad esempio, di spamming. Lo "spammatore" ha infatti bisogno di un gran numero di indirizzi e-mail da cui far partire i propri messaggi; a questo scopo utilizza robot che,in automatico, vanno a "rubare" dai vari fornitori di servizi di posta online, quali Hotmail, Libero, Tiscali eccetera indirizzi utili allo scopo. Un'altra applicazione utile dei Captcha è legata al controllo delle interrogazioni ai siti. Richieste frequenti, quali ad esempio l'invio abnorme e ripetuto di messaggi a un forum, potrebbero mettere in difficoltà la capacità di elaborazione del server provocando, di fatto, conseguenze simili a un attacco DoS.

In sostanza i Captcha hanno la funzione di assicurarsi che dietro a ogni richiesta a un server ci sia una persona pensante e non un robot maligno, da qui il nome che in inglese significa: "completely automated public turing test to tell computers and humans apart" (test pubblico e completamente automatico per distinguere computer e umani).

Malgrado la presenza dei Captcha, servizi come Hotmail o Gmail continuano ad essere attaccati. Da una recente indagine sembra addirittura che la percentuale di successo degli attacchi a Hotmail sia compresa tra il 10 e il 15%.



Il trucco per superare l'ostacolo, in teoria, è semplice: creare dei programmi che, come se fossero degli OCR superintelligenti, siano capaci di interpretare i Captcha, permettendo di superarne il filtro senza l'intervento umano.

:: Come funzionano

Vediamo cosa deve fare un programma per decodificare un Captcha di tipo testuale (ne esistono anche di tipo vocale):

- **Riduzione dei disturbi di fondo** Consiste nel rimuovere tutti i frammenti di informazioni inutili e ridurre i colori dello sfondo. Di solito, immagini spezzate o che non hanno nessuna possibile corrispondenza con interse-

zioni di lettere o numeri esistenti vengono scartate e cancellate dallo sfondo.

- **Suddivisione logica**
  Sull'immagine ripulita, a questo punto, avviene la suddivisione logica degli elementi.
- **Identificazione**
  L'ultima fase si basa fondamentalmente sui paragoni tra forme e sulla relativa compatibilità delle varie lettere e numeri con queste forme.

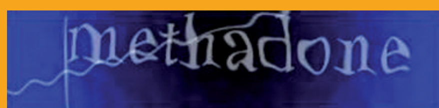
Risultati di questo genere sono già stati raggiunti da diversi programmi. Tra i più famosi troviamo Xrumer Conjecture (derivato dal noto GOCR),che oltre a simulare il comportamento di un utente standard, creando ad esempio post sui forum, è appunto in grado di interpretare i Captcha difensivi di Gmail, e PWNtcha, molto semplice da usare a livello di implementazione e di programmazione, capace di decodificare specifici Captcha.

:: La battaglia continua

Ed è proprio in considerazione della relativa semplicità con cui si riesce a crackare un Captcha testuale che si stanno cercando soluzioni differenti da cifre e caratteri deformati.
Alcuni sviluppatori stanno lavorando in direzione della interpretazione delle immagini, ad esempio proponendo foto in cui appaiono un ippopotamo, un canarino e un



L'interfaccia di Asirra: se decidiamo di adottare un gattino facendo clic sul link, la procedura viene annullata e dovremo ripetere la selezione.





gatto e chiedendo all'utente di rispondere a una domanda inerente questi animali. Ma anche in questo settore sta scendendo in campo l'incredibile potenza dell'Intelligenza Artificiale. Philippe Golle, ricercatore del famoso Palo Alto Research Center, ha spiegato come una AI, addestrata a dovere, sia in grado di arrivare a risultati impensabili. Il ricercatore ha dimostrato che è possibile violare la nuova tecnologia grafica di Microsoft (Asirra) addestrando l'AI a distinguere il contenuto delle immagini proposte dal sistema. In un test effettuato con un software che usa principi simili a quelli della Microsoft, si propongono al visitatore alcune immagini di animali, provenienti da un database di milioni di foto, e gli si chiede di distinguere tra razze e varietà di felini o canidi. Golle ha dimostrato che la barriera non è insormontabile per un computer. Già ora, dopo varie prove, il suo software è riuscito a distinguere le foto di cani da quelle di gatti.



Per ottenere questo risultato sono state utilizzate avanzate tecniche capaci di riconoscere le forme prendendo in considerazione anche la posizione delle stesse, le loro proporzioni e i colori. Ad esempio, la presenza del colore rosaceo nelle dimensioni della lingua di un cane potrebbe essere un fattore discriminante per scartare la possibilità che si tratti di un gatto. Oppure, al contrario, la presenza del colore giallo degli occhi abbinato al nero del mantello, potrebbe identificare un gatto a discapito di un cane. Discorso analogo per la presenza dei denti, che normalmente nei gatti non viene mostrata. Gli studi e le prove di Golle intanto proseguono e il sistema continua a imparare; fino a che punto riuscirà ad arrivare lo scopriremo presto.

IL TEOREMA DI BAYES

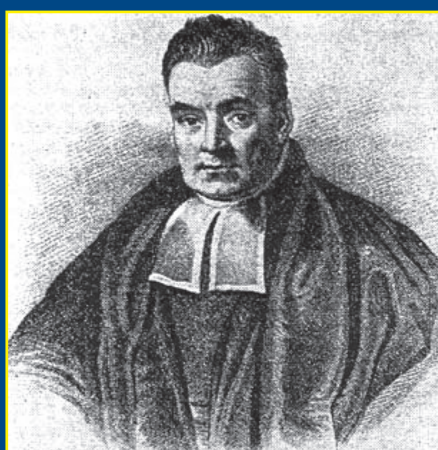


Molti pensano che il filtro Bayesiano si basi su un moderno algortitmo. Niente di più sbagliato

Il filtro, considerato da molti la più efficace soluzione al problema dello spam, si basa su un teorema legato al calcolo delle probabilità sviluppato nel lontano 1700 dal matematico inglese Thomas Bayes; L'omonimo teorema si basava, a sua volta, su altri due teoremi riguardanti anch'essi le probabilità: il "teorema della probabilità composta" e il "teorema della probabilità assoluta". A distanza di 300 anni, questo teorema trova la sua applicazione pratica nella realizzazione dei più moderni filtri anti spam.

:: Standard & Bayesan

Alzi la mano chi, malgrado la presenza di un programma antispam sul proprio computer, non abbia continuato a ritrovarsi la mail intasata di posta spazzatura e allo stesso tempo non si sia ritrovato cestinate mail importanti.
Il principale problema dei filtri "standard" è che questi utilizzano, per poter distinguere lo spam dalle email corrette, sostanzialmente solo una lista di parole chiave. Fatta la legge trovato l'inganno, ed ecco che gli spammer hanno cominciato a scrivere "v-i-a-g-r-a" invece che "viagra", imbrogliando in questo modo i software e costringendo i programmatori a una continua corsa all'aggiornamento dei database di parole chiave. La nuova tendenza è quindi quella di sviluppare filtri capaci di "calcolare" la probabilità che una mail sia o no spam.



Il teorema di Bayes (1702-1761) fu pubblicato postumo nel 1763 su Philosophical Transactions of the Royal Society of London.

Ed è proprio qui che entra in gioco il teorema di Thomas Bayes.

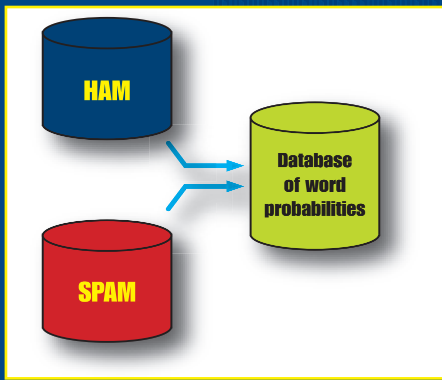
:: Il pro...

Il principio di base è apparentemente semplice: aggiungere all'elenco di parole chiave lo studio delle ricorrenze tra le stesse, ovvero analizzare le sequenze di parole, messe nello stesso ordine o nello stesso contesto, per determinare se una email sia spam o meno.
Ad esempio, sempre per rimanere in tema di viagra, se in una email compare la parola "viagra" e "acquista" e "online", al 99% stiamo parlando di una mail spam. Esattamente al contrario di un testo come: "Sai Morgoth non so come fare con tutte queste email che ricevo sul viagra, puoi aiutarmi?". Se utilizzassimo un filtro basato sul semplice elenco di parole, non riceveremmo mai questa richiesta d'aiuto, mentre un filtro bayesiano ne saprebbe sicuramente riconoscere la validità.
Ne consegue che, per poter funzionare, questi sistemi necessitino di un database contenente sia le parole ricorrenti nelle email spam, sia in

quelle corrette: il database delle casistiche. Come ogni buon programma intelligente, questi sistemi ricordano le scelte fatte dall'utente per elaborare le successive valutazioni. Infine, l'intero corpo della mail, quindi anche le voci nell'headler , vengono prese in considerazione, costringendo lo spammer a cambiare mailer a ogni invio

:: ...e il contro

Similmente ai firewall che "apprendono" quali applicazione permettere e quali no, anche i sistemi bayesiani continuano a interrogare l'utente sul comportamento da tenere con questa o quell'altra email. Una scocciatura che spesso diventa più noiosa del dover cancellare la stessa posta spazzatura. Armiamoci quindi di un poco di pazienza e istruiamolo a dovere; fortunatamente, come con i firewall, questo periodo di training è limitato nel tempo. Molti programmi dispongono di addestramenti pre-confezionati; niente di più inutile, il vantaggio di questa tecnologia sta proprio nella personalizzazione. Facciamo un altro esempio: una azienda che si occupa di viaggi potrebbe ricevere molte email contenenti la parola "republic" inclusa nei vari programmi turistici della "repubblic of congo". Essendo "republic" una delle maggiori chiavi usate per identificare lo spam, queste email vengono bloccate dai filtri standard, mentre nel caso del filtro bayesiano, la creazione dell'apposita regola ne permette il passaggio.



I database delle casistiche è il fulcro del sistema bayesiano.

Se più messaggi simili hanno le stesse parole ricorrenti, la regola prende un profilo sempre più preciso fino a raggiungere una deduzione corretta nel 95%. Non male!

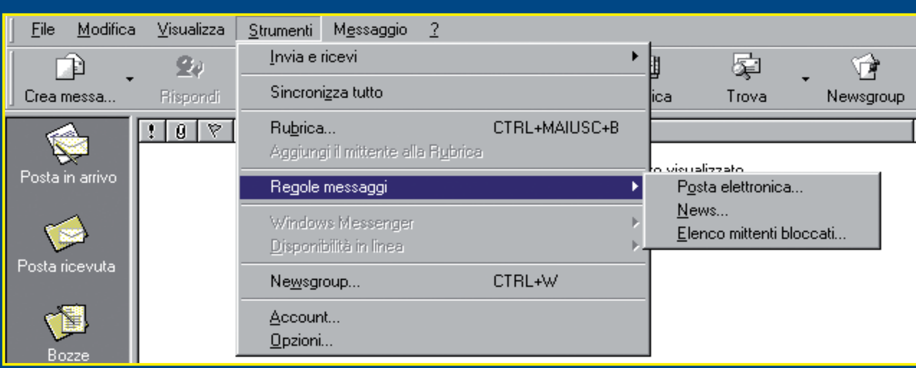
:: L'altra faccia della medaglia

Non esistono soluzioni perfette o tantomeno invincibili, anche i programmi che utilizzano il filtro bayesiamo sono vulnerabili. Mettiamo il caso di aver ricevuto un numero consistente di email da un determinato indirizzo o con un certo contenuto, e averle considerate attendibili creando l'apposita regola, le mail spam che arrivassero successivamente da quell'utente o con quello stesso contenuto verrebbero lasciate passare per un certo periodo di tempo, fin quando il valore dell'indirizzo o del contenuto, definito dalla regola iniziale non spam, non diventi inferiore al valore della nuova regola che lo definisce spam.

:: Riassumendo

I vantaggi del filtro bayesiano sono:
1) Approccio di tipo relativo e selettivo in base a casistica e non semplice presenza di una parola;
2) Aggiornamento continuo, grazie alla procedura di apprendimento, sia delle chiavi sia alle nuove tecniche di spam;
3) Massima personalizzazione;
4) Poliglotta, non essendo legato esclusivamente all'elenco di chiavi non richiede aggiornamenti di dizionari nelle varie lingue (lo spam non ha frontiere).

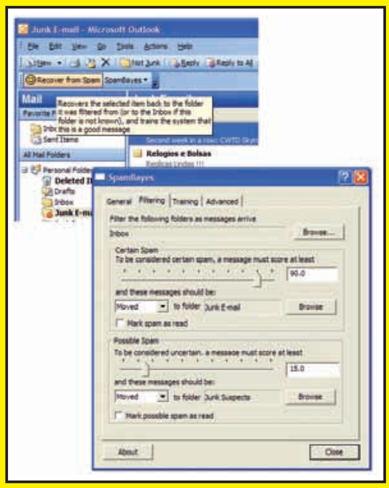
Morgoth



All'inizio il programma ci tempesta di richieste, come un bambino che impara a parlare e chiede continuamente: "cos'è? "Perché?".

QUALI SOFTWARE

Una delle migliori soluzioni, rigorosamente Open Source, per provare la potenza del filtro bayesiano è SpamBayes (http://spambayes.sourceforge.net/) giunto alla versione 1.0.4 e compatibile con i principali account di posta elettronica come Gmail, Yahoo! Mail e MSN Hotmail, con il "nostro" Thunderbird e con gli immancabili Vista e Microsoft Office 2007 dare sul sito di Privnote.





WEB MARKET

Come il diavolo commerciale ha conquistato il paradiso della Rete

Poco tempo fa mi è stato regalato un vecchio notebook mal funzionante, per vedere se riuscissi a ricavarne qualcosa. Individuato il modello esatto ho lanciato il browser e digitato marca e sigla alla ricerca di qualche informazione in più.

:: Comprami, io sono in vendita

Nulla. Le prime due pagine di Google erano zeppe di collegamenti verso siti che vendono batterie e memorie di ricambio per quel computer . Poi, seminascosto tra gli altri solamente in terza pagina, ho scovato un collegamento a una pagina del servizio di assistenza clienti del produttore dove finalmente ho potuto trovare le informazioni che mi servivano.
Ma diamine, mi son detto, perché questo non appare per primo nella ricerca?Internet non dovrebbe essere la fonte primaria di informazioni? Che domande baby: è l'anima commerciale che ha conquistato il Web.
Il guaio è che non solo Google , ma bene o male tutti i motori di ricerca sono affetti da questo: all'inizio della ricerca e ben visibili solo collegamenti a scopo commerciale, tutto il resto delle informazioni viene dopo.

:: Un po' di storia

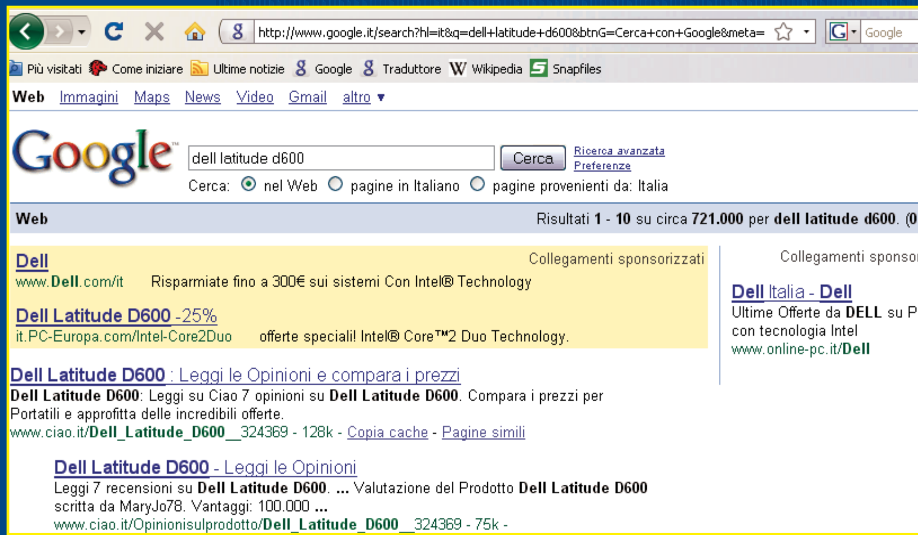
Agli albori del Web le informazioni disponibili online erano limitate, in genere bastava raggiungere il sito desiderato e qui cercare le informazione sfogliando i menu interni. Ma il Web è cresciuto molto velocement.Vecchi siti muoiono, nuovi ne vengono creati ogni giorno e le informazioni cambiano sede o forma e purtroppo talvolta finiscono per essere dimenticate perché obsolete. In questo marasma di cambiamenti si è pensato quindi di creare dei sistemi di indicizzazione per guidare le ricerche. Così sono nati i primi motori di ricerca, inizialmente semplici directory (database di siti compilati per lo più a mano in base a segnalazioni). Questo sistema ha funzionato per un breve periodo di tempo: le informazioni da catalogare erano ingenti, le risorse (intese come tempo e come forza lavoro) troppo poche.
La soluzione è stata quella di automatizzare il più possibile il processo, sviluppando dei software denominati spider. Uno spider (ragno in inglese) non è altro che un robot, un software che funziona autonomamente, che parte da un indirizzo dato e scorre tutti i collegamenti che trova, catalogando in un database il contenuto delle pagine incontrate. Quando effettuiamo una ricerca sul Web, accediamo alle informazioni inserite nel database del motore proprio da questi programmi.

:: L'approccio di oggi

In realtà non si tratta di una cosa nuovissima, un po' come la scoperta dell'acqua calda: ho uno spazio che permette a chi naviga di trovare un sito tra milioni, perché non far pagare le aziende perché il loro sito venga mostrato tra i primi risultati delle ricerche? Da un punto di vista commerciale è un'idea geniale, ma la cosa è stata scoperta quasi subito, pareva infatti impossibile che ogni ricerca riportasse sempre a siti con interessi commerciali piuttosto che ad approfondimenti sui termini cercati. Sotto la pressione del pubblico e delle authority, quindi, i vari Google, Yahoo, Altavista e così via hanno dovuto indicare chiaramente quando un sito proposto è in realtà un'inserzione pubblicitaria (in Google lo vediamo perché questi siti sono visualizzati con sfondo colorato ed è indicato che si tratta di "collegamenti sponsorizzati"). Va bene, ma noi continuiamo a trovare pagine e pagine di collegamenti a siti commerciali e le informazioni che ci interessano sono sempre più relegate in secondo piano. Perché?

:: Squali tra i naviganti

La colpa dei motori di ricerca è forse quella di aver "dato il La" alla trasformazione del Web in un grande supermercato online: sul Web si guadagna, e anche bene, quindi la proliferazione di siti commerciali avviene a un tasso molto maggiore di quella dei siti puramente informativi. Se prima erano i motori di ricerca ad esaltare i siti commerciali nei risultati, ora non c'è n'è più bisogno, perché sono talmente tanti che gli spider devono passarne migliaia prima di trovare un sito informativo. Logico quindi che i loro database strabordino di siti che cercano di venderci ciò che abbiamo cercato e non di informarci su di esso. E gli spider non fanno altro che il loro mestiere: scorrono la Rete e catalogano quello che trovano.



Ricerchiamo un modello di notebook con Google per trovare informazioni sulla sua struttura e sul servizio assistenza del produttore, ma non siamo fortunati...

:: La nostra difesa

Non serve subire passivi questa tendenza al commerciale del Web, a meno che non siamo in effetti interessati all'acquisto di qualcosa. Esistono tecniche di ricerca che ci permettono di filtrare, e di molto, i risultati ottenuti dai contenuti prettamente commerciali, ed è buona cosa impararle se non vogliamo diventare zombie della carta di credito. Innanzitutto, impariamo i comandi che possiamo inserire nella casella insieme ai termini da cercare per limitare e filtrare il più possibile le informazioni mostrate. Per esempio il segno meno: se lo inseriamo subito prima di una parola, tutti i siti che la contengono verranno lasciati fuori dai risultati. In secondo luogo, iniziamo a variare l'origine delle nostre ricerche in base a ciò che stiamo cercando: per informazioni di cultura generale è meglio partire da Wikipedia e seguire al limite i collegamenti esterni proposti.
La Rete è fatta soprattutto da persone che la percorrono e la popolano quotidianamente, non da aziende commerciali e da robot; se cerchiamo la soluzione a un dato problema, cerchiamola in un newsgroup e non sul Web, sarà più facile trovare qualcuno che l'ha già trovata prima di voi.



Con Yahoo va un po' meglio, abbiamo sempre link sponsorizzati all'inizio dei risultati, ma anche il collegamento verso quello che ci interessa.

INTERNET KO

Scoperta una tecnica che consente di effettuare facili hijacking del traffico-dati



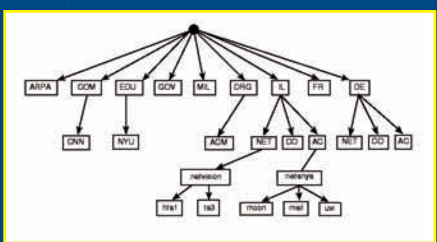
Immaginiamo di edificare un palazzo su delle fondamenta gettate da un'altra persona, che ci rassicura sulla loro solidità.
Dopo qualche anno, scopriamo che le fondamenta sono di un materiale molto fragile, che mette a serio rischio la sicurezza dell'edificio. Che cosa facciamo? Continuiamo come niente fosse, incrociando le dita; oppure abbandoniamo il palazzo, lo radiamo al suolo e lo rifacciamo nuovo di zecca (con nuove fondamenta, è chiaro)?
Questa è, più o meno, la situazione che sta vivendo Internet in queste settimane, dopo che gli esperti di sicurezza Anton "Tony" Kapela e Alex Pilosov, durante il recente DefCon 16 (http://www.defcon.org), hanno dimostrato una tecnica in grado di deviare un traffico di dati a una postazione intermedia con la possibilità di spiarlo o, addirittura, modificarlo. Insomma, un "eavesdropping" a tutti gli effetti. Sai che novità, direte voi. Attenzione, la notizia bomba deve ancora arrivare: la tecnica si basa su un utilizzo "alternativo" del Border Gateway Protocol (BGP). Sì, proprio lui: il protocollo di routing che gestisce forse la parte più intima e vitale di Internet. E non parliamo della scoperta di chissà quale bug, come conferma Kapela: "Non stiamo facendo niente fuori dall'ordinario". E aggiunge: "Non ci sono vulnerabilità, errori di protocollo, non ci sono problemi di software. Il problema deriva dal livello di interconnettività richiesto per far sì che tutto funzioni". E quanto ha ragione, il buon Anton. Il problema, infatti, si basa sulla natura stessa del BGP, che non contempla azioni malevole. Ma andiamo con ordine...



I due ricercatori presentano la scoperta al DefCon 16 del 15 ottobre.

:: Colpa di una tabella

Quando digitiamo un indirizzo web nel browser, e premiamo Invio, il Domain Name System (DNS) lo traduce nel corrispettivo indirizzo IP.
A questo punto, un router del nostro fornitore di accesso a Internet (l'ISP) non fa altro che consultare una tabella del BGP, alla ricerca del percorso più veloce, per metterci in contatto con quel dato IP. Insomma, un po' come consultare uno stradario web alla ricerca dell'itinerario più breve. Il problema è che questa tabella è compilata sulla base di "dichiarazioni" effettuate dagli altri ISP e "AS" (Autonomous System) che dichiarano volontariamente le fasce di IP che gestiscono.

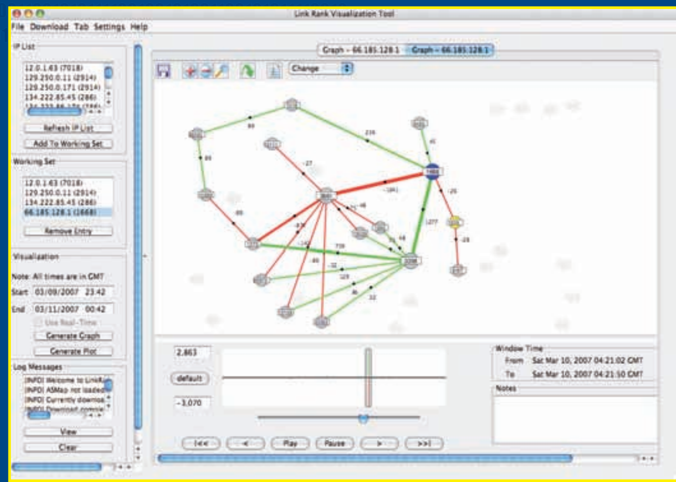


Uno schema semplificato del funzionamento del Domain Name System.

Se due AS dichiarano di gestire il medesimo IP, è considerato "idoneo" quello più specifico; cioè con più subset dell'indirizzo desiderato. La fregatura sta nella dichiarazione degli indirizzi IP da parte degli Internet Service Provider, che viene sempre e comunque considerata veritiera.

:: Il colpevole? Sconosciuto!

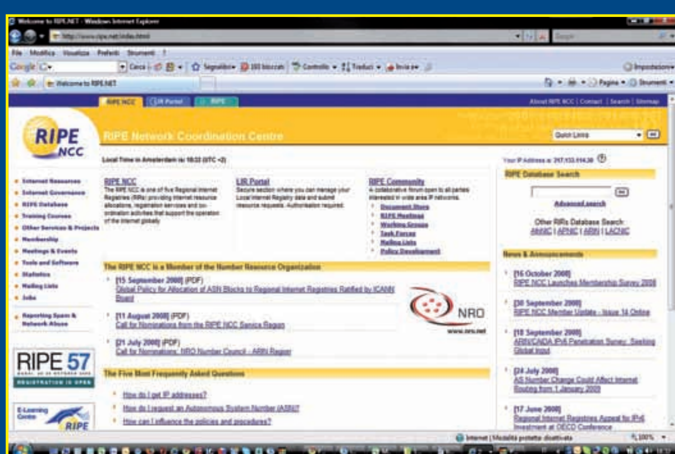
Quindi, in buona sostanza, per eseguire un "evesdropping", a un criminale informatico è sufficiente dichiarare una fascia di indirizzi IP più specifica rispetto agli ISP tradizionali, che diventano veri e propri "concorrenti". Naturalmente, il criminale può indirizzare i suoi interessi verso un preciso IP, che magari tiene d'occhio da diverso tempo. Si tratta a tutti gli effetti di un classico "IP hijack", con la differenza che si effettua senza sfruttare alcuna debolezza del sistema attaccato: si tratta "solo" di utilizzare Internet, come farebbe un qualunque ISP. In questo modo, tra l'altro, le possibilità di smascherare il colpevole sono ridotte al lumicino, perché un "evesdropping" di questo tipo è difficilmente intercettabile: l'instradamento del traffico di dati, verso il sistema del criminale informatico, rappresenta in fondo solo una piccola deviazione; equivalente a un ritardo di pochi millisecondi nella risposta del vero IP di destinazione.



Possiamo ancora scaricare gratuitamente la versione 1.0 del programma. La versione 2.0 è prevista per la fine di dicembre.

:: Invisibili come non mai

Una vera e propria tecnica "stealth", insomma, come confermato dalle ricerche di alcuni esperti dell'Università dell'Oregon.
Utilizzando il software dedicato LinkRank (http://linkrank.cs.ucla.edu/), si sono messi di buona lena e hanno analizzato una moltitudine di traffici di dati, sia "deviati" che non. E il risultato, allarmante, è che senza possibilità di risalire a un contesto specifico, è molto difficile distinguere una deviazione legittima da una frutto di un hijacking. Dopotutto, le deviazioni sono un evento frequente nel traffico di dati, e scatenato da svariati fattori.



RIPE NCC (www.ripe.net) è uno dei cinque RIR che gestiscono le risorse Internet a livello mondiale.

:: La soluzione (forse) c'è

Una sconfitta irreparabile, dunque, per l'architettura su cui poggia l'intera Rete mondiale?
Non proprio, perché, stando sempre alle dichiarazioni di Kapela, prevenire un hijacking di questo tipo è possibile; anche se non facile. In pratica, occorre che tutti gli ISP stabiliscano fasce di indirizzi IP "autenticati", dei quali si possono fidare e che possano essere preposti alla deviazione del traffico dati, quando necessario. Si tratta però di un lavoro enorme, lungo e laborioso; e che richiede la partecipazione di tutti gli ISP. Se solo uno non accetta questo compromesso, si bloccherebbe tutto il processo.
Un metodo in teoria più semplice consiste nel fare in modo che i cinque Regional Internet Registry (RIR), mondiali certifichino le fasce di indirizzi IP gestiti a tutti gli ISP; di modo che possano essere di volta in volta verificate le varie "dichiarazioni". Non si tratta di uno scherzetto nemmeno in questo caso, ma dopotutto è sempre meglio di staccare la spina a Internet e attaccare il cartello di "lavori in corso" per i mesi a venire. O no?

Riccardo Meggiatto

C:\>_ERANO UNA VOLTÀ LE BBS



Quando Internet era solo un'idea pochi coraggiosi si scambiavano già messaggi e informazioni

Il sistema delle BBS si basava su una linea commutata; in parole povere si utilizzavano dei modem che gestivano la comunicazione dati tra due computer. Quando il sistema prese piede in Italia si viaggiava alla velocità di 2400bds e solo i più "sfigati" avevano modem a 1200bds o addirittura 300bds!
Alcuni gestori avevano configurato la propria BBS per rifiutare connessioni a 300 o a 1200bds, insomma delle vere e proprie BBS elitarie.
Eccola qui, la famosa parola BBS, che è acronimo di Bullettin Board System, ovvero un sistema telematico per lo scambio di messaggi.

:: Cos'erano

Una BBS era fondamentalmente costituita da un computer, che oggi chiameremmo server, attaccato alla linea telefonica tramite un modem. Quasi tutte le applicazioni erano DOS o al massimo OS2 (il sistema operativo dell'IBM che consentiva il multitasking). Ogni BBS gestiva 1 solo modem, quindi una connessione alla volta. Ciò significa che, calcolando una connessione media di 30 minuti, si potevano avere al massimo 48 accessi, sempre che le connessioni si verificassero spalmate in tutte le ore. Come detto, alcune BBS erano dotate di sistemi multitaskingcomputer dotati di 4 porte seriali consentivano di avere un numero potenziale di 4 modem. Ma voleva anche dire che, acquistati i modem si dovevano pagare alla monopolista Telecom Italia i relativi abbonamenti al telefono fisso.

:: Le prime Chat

La BBS consentiva a più utenti di trovarsi online e, tramite un sistema per certi versi migliore delle attuali chat, gli permetteva di comunicare tra di loro. Vi erano anche basi messaggi con vari temi. I messaggi potevano essere letti online (pagando la telefonata per tutta la durata della connessione) oppure si potevano scaricare in locale e leggere con tut-



Un altro utente si collega a un'altra BBS dello stesso Net.

ta calma; quest'ultimi si chiamavano, per l'appunto, Offline-Reader. Tutte queste operazioni erano compiute su scelte precise fatte dagli utenti durante la "navigazione", ma vi era un altro sistema: quello automatizzato che usavano le BBS stesse. La tecnologia FidoNet, su cui si basava anche la rete RingNet, aveva una struttura ben precisa e serviva per mettere in comunicazione tutte le BBS d'Italia e del mondo. I SysOp (System Operator ovvero proprietari delle BBS) spesso si univano in organizzazioni per poter dare ai propri utenti questo tipo di servizi.
Il tutto avveniva in maniera gratuita, al massimo veniva accettata una donazione che andava interamente investita nei costi di abbonamento alla linea telefonica e per l'acquisto e aggiornamento dell'hardware. Il sistema di scambio messaggi tra BBS aveva vari livelli di efficienza.
Vi erano network che garantivano una base messaggi aggiornata con cadenza giornaliera, altri ogni due giorni, altri ancora settimanale.

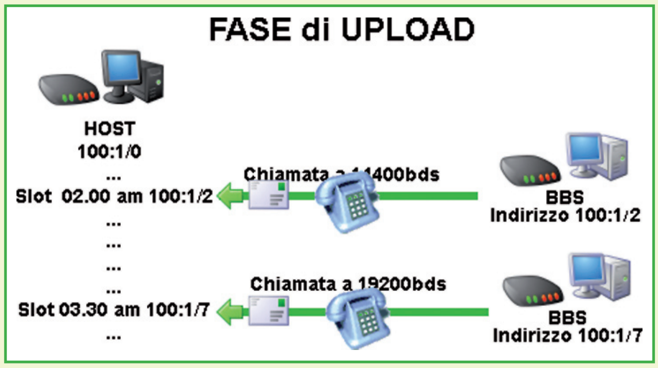
:: Come funzionavano

Il sistema funzionava così: L'utente A si collegava a una BBS della rete RingNet, ad esempio 100:1/2 (Milano). Consultava i messaggi e scriveva in risposta a B che invece si collegava alla BBS Nodo 100:1/7 di RingNet (Firenze).

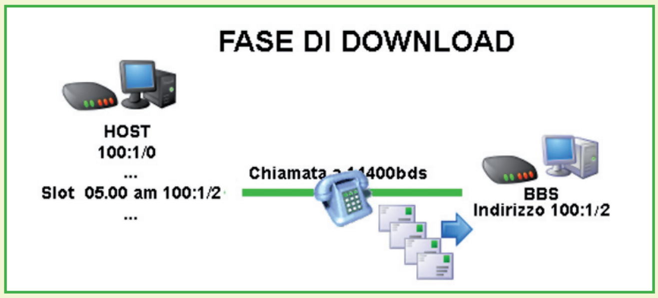


Collegamento diretto tra utente e BBS.

I due utenti non dovevano collegarsi necessariamente nel medesimo istante. Tutto il network era scrupolosamente organizzato in slot per la sincronizzazione dei sistemi, tanto che in determinati orari le BBS rifiutavano le connessioni degli utenti per effettuare quelle puramente "tecniche" di sincronizzazione, in cui veniva effettuato un packing con ARJ di tutti i messaggi da inviare al proprio hub.



Le varie BBS inviano i messaggi a un nodo centrale.



Le BBS scaricano la posta dal nodo centrale.

Ogni nodo della rete si presentava al suo hub o host e inviava il pacchetto ottimizzando al massimo il tempo di connessione e quindi i costi. Difficile che una connessione durasse più di un minuto anche con carichi notevoli di messaggi. Chi non rispettava gli slot, probabilmente non riusciva a sincronizzare la posta. Poi l'host, in questo caso il 100:1/0, rielaborava tutte le aree messaggi, preparava i pacchetti personalizzati per ogni nodo e li comprimeva mettendosi poi in attesa di altre chiamate per il pickup della posta. A questo punto il nodo 100:1/2 si ricollegava e aveva la situazione aggiornata alla sera prima e B poteva leggere il messaggio di A dal nodo di Milano.

:: Le SubNet

La rete era divisa in SubNet che si differenziavano per l'indirizzo. Questo sistema, molto simile all'indirizzo IP, aveva la possibilità di identificare e quindi reindirizzare ogni messaggio verso il corretto destinatario. Naturalmente in caso di messaggi privati (matrix) le BBS interessate erano solo BBS mittente, BBS hub e BBS destinataria. A volte erano permessi invii immediati dove BBS mittente contattava e consegnava la matrix direttamente al sistema destinatario, ma era un sistema troppo costoso.
Per gestire tutti questi sistemi e per sapere i numeri di telefono delle BBS c'erano delle nodelist, ossia liste di nodi, fondamentali per la corretta gestione e inoltro delle informazioni. Le nodelist erano pubblicate su riviste di settore, il più delle volte erano elenchi compilati a mano.
E furono proprio questi elenchi a scatenare il famoso Crackdown del 1994 ad opera della Guardia di Finanza.

Prendere la giusta direzione nei videogiochi è una questione di... matematica!

SI FA PRESTO A DIRE "VAI LÌ"

Se qualcuno ci chiedesse il percorso da prendere, per spostarsi dal punto in cui si trova a uno che sta cinque metri di fronte, lo guarderemmo di certo sbigottiti. Anzi, forse cercheremmo con nonchalance il telefonino per avvertire la Polizia che, da oggi, c'è un pazzo in più sulla strada. Presuntuosi: il cervello umano è così potente e raffinato che, quando le distanze sono così ridotte, il calcolare il percorso da un punto A a un punto B diventa un gioco da ragazzi. In realtà la situazione non è mai così apertamente semplice. Mettiamo per esempio che in mezzo a questo ipotetico tragitto si trovi un albero. Non ci sogneremmo mai e poi mai di spiegare al nostro interlocutore che per arrivare al punto B deve prima girarci intorno. Insomma, viene automatico pensare che sia un



processo scontato. Sì, certo, scontato per noi. Ma se fossimo così ingenui, quando si tratta di spiegare il percorso a un'unità nel nostro videogioco strategico preferito, le cose andrebbero diversamente, garantito! Come minimo, il nostro bel "Predator Battle Tank" di Command and Conquer 3, o una jeep di Company of Heroes, centrerebbe in pieno quell'albero. E le cose non andrebbero diversamente col nostro eroe in Diablo II, malgrado sia un classico gioco di ruolo. I videogiochi, come del resto tutte le simulazioni informatiche (anche quelle "serie"), basano ogni loro spostamento su complesse procedure matematiche, gli **algoritmi**, che non possono prescindere da qualunque elemento utile per calcolare anche un percorso di estrema semplicità. Tanto è vero che questa operazione, in apparenza banale, è una delle branche più sviluppate e al tempo stesso più affascinanti di quella che chiamiamo "intelligenza artificiale". Proprio così: quando diciamo che un videogioco strategico ha una buona intelligenza artificiale, anche se non ce ne rendiamo conto, stiamo affermando che le nostre unità calcolano nel modo più opportuno il percorso necessario a raggiungere i punti che di volta in volta indichiamo loro. Similmente, una buona intelligenza artificiale prevede che anche gli avversari gestiti dal computer



siano dotati di una capacità "credibile" nel calcolare un percorso. Come dire, insomma, che essere intelligenti è una questione d'orientamento.

:: Anche i computer barano

Se siamo giocatori di vecchia data, ricorderemo la grande frustrazione che provavamo nel giocare a titoli strategici come "Dune" e il primissimo "Warlord", per non parlare di quelli venuti prima. In questi videogiochi il computer aveva un vantaggio notevole: sapeva, a priori, dove ci trovavamo nella mappa. Insomma, in questi casi buona parte dell'intelligenza artificiale consisteva nel ritardare il momento dello scontro in modo realistico, e non nel passare tempo, mezzi e analisi per scovarci. È una differenza forse sottile ma fondamentale: a un computer che sa dove ci troviamo fin dall'inizio della partita, basta un'intelligenza artificiale stupida. Se invece non sa dove ci troviamo e deve giocoforza sfruttare le proprie risorse per trovarci, come del resto facciamo noi, deve avere una buona intelligenza artificiale. Tutto ciò che viene dopo, incluse le tattiche che stabiliscono le formazioni delle unità o le strategie utilizzate nella raccolta delle risorse, è strettamente legato a questo aspetto che scavalca le barriere videoludiche per approdare ad avanzate applicazioni legate alle simulazioni militari, industriali e scientifiche. Pensiamo a quei robot automatici in grado di effettuare la ricognizione di un campo di battaglia senza l'ausilio del controllo umano. In questi casi è necessaria un'intelligenza artificiale estremamente evoluta, specialmente nel calcolo del percorso ideale per scovare il nemico senza essere visti. Un sistema di sensori deve occuparsi di rilevare le presenze ostili e, in base ai dati ottenuti, calcolare un percorso che sia al contempo sicuro e che permetta di accertarsi della loro entità. E qui entra in





gioco (è proprio il caso di dirlo) un'intelligenza artificiale fortemente basata sugli "Algoritmi di ricerca del percorso". Una definizione che fa paura solo al pronunciarla al punto che, per semplicità, si è soliti parlare di "pathfinding". Un po' di deja vu?

:: Dalla Terra a Marte

Se non siamo totalmente estranei alle cronache scientifiche e tecnologiche, di sicuro abbiamo sentito parlare di "Pathfinder".
È la sonda che si sta muovendo sulla superficie di Marte, per studiarla. Anche in questo caso, la ricerca dei percorsi ideali è fondamentale per la riuscita della missione. Si fa presto a pensare che, per raggiungere un punto che si trova appena un metro più avanti, la sonda debba solo procedere secondo una traiettoria rettilinea. In fondo si tratta del percorso più breve, no? Ma se in quel metro si trovasse, per esempio, una fossa? O se proprio in mezzo a quel tragitto ci fosse un qualsiasi tipo di ostacolo? La sonda vi si incastrerebbe, mandando in fumo i sogni di gloria e di conquista spaziale (oltre che milioni di euro). Nel pathfinding quindi, il percorso "ideale" non necessariamente quello più breve, bensì quello più "opportuno", sulla base di una lunga serie di fattori. Più lunga e dettagliato è l'elenco di fattori preso in considerazione, migliore sarà l'algoritmo di pathfinding utilizzato da quella specifica applicazione, sia che si tratti del software che comanda un sonda, sia che si tratti dell'l'intelligenza artificiale che gestisce le unità di un videogioco. Detto tutto ciò, gli utilizzi viedoludici rimangano all'avanguardia in questo settore, e non è un mistero che i più grandi esperti d'intelligenza artificiale provengono dal mondo che ha dato i natali a Wacraft, Command & Conquer, Empire Earth, Civilization e via dicendo.



:: Questione di "peso"

Una delle tecniche di pathfinding più semplici ma al tempo stesso efficaci, utilizzate in molti videogiochi strategici, si basa sul così detto "peso".
Immaginiamo innanzitutto che la mappa di un ipotetico gioco strategico sia suddivisa in caselle. In ogni casella trova posto un certo tipo di superficie. Mettiamo il caso che alcune caselle attigue rappresentino un lago, altre invece, in questo caso anche separate tra loro, rappresentino degli alberi; in alcune caselle troviamo del semplice terreno solido mentre in altre ancora del terreno fangoso. Ora, poniamo che la nostra unità si trovi in un determinato punto della mappa e che giunga il momento di assegnarle un nuovo punto di destinazione. In questo caso, l'intelligenza artificiale assegna un diverso "peso" alle varie caselle, in base al tipo di superficie. Per esempio, al terreno solido e secco è dato un peso di 1, al fango un peso di 2, alla roccia un peso di 3. A caselle insormontabili (a meno che non si disponga di qualche veicolo speciale, ma qui intervengono altri parametri) sono assegnati invece dei valori molto più alti. Per esempio 100 alle caselle con alberi e a quelle con acqua. A questo punto, l'algoritmo di pathfinding elabora tutti i possibili percorsi calcolando il peso di totale di ognuno e scegliendo alla fine quello più leggero.
Ad esempio, se un percorso è formato da 40 caselle di terreno solido e secco (1 x 40 = 40) sarà preferito rispetto

a uno composto da 15 caselle di roccia (3 x 15 =45). Se poi c'è di mezzo un albero, o dell'acqua, il peso del percorso si alza a dismisura.

:: E ora, mettiamoci un nemico

Questo calcolo di base viene poi arricchito di altri elementi come la presenza, o meno di un'unità nemica in una delle caselle che compongono il percorso scelto: anche in questo caso la questione viene riportata al calcolo del "peso". L'intelligenza artificiale è messa di fronte a una scelta: rischiare lo scontro, oppure cambiare tragitto preferendo quello più pesante? In questo caso l'algoritmo deve compiere ulteriori valutazioni: innanzitutto, attribuisce un valore alla differenza tra la forza dell'unità nemica e la nostra. In caso di valore positivo, ovvero se l'unità nemica risultasse più forte della nostra, nella relativa casella viene aggiunto ulteriore "peso", modificando di conseguenza anche il peso totale del percorso. A questo punto vengono comparati nuovamente il nuovo valore del percorso scelto inizialmente con quello del percorso roccioso e se quest'ultimo risultasse più leggero ecco che l'algoritmo aggiorna la sua scelta. In questi casi esiste anche la possibilità di "mixare" i dati rilevati.



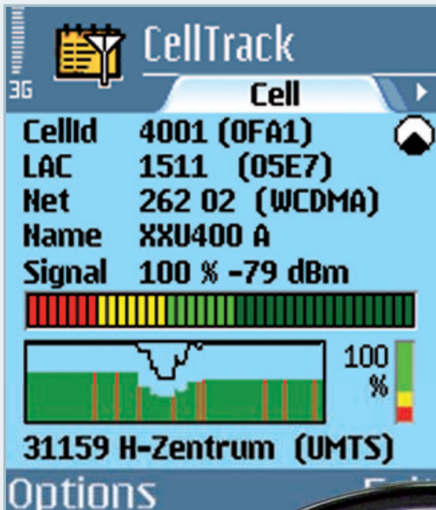
Per esempio, se l'intelligenza artificiale è ben strutturata, può prevedere di far marciare l'unità per qualche casella sul terreno iniziale, quindi deviare sul sentiero di roccia evitando il nemico, per poi tornare sui suoi passi. Un ulteriore aggiunta, ma qui si va su tecnologie software estremamente raffinate, consiste nella valutazione delle condizioni climatiche.
Torniamo sui nostri due percorsi, uno di terreno solido e secco e uno di roccia; mettiamo che sul primo si abbatta un violento nubifragio. L'intelligenza artificiale evoluta, considererà il fatto che il terreno, originariamente duro e secco, si è trasformato in fangoso; e dunque dovrà variare il "peso" delle caselle, passandolo da 1 a 2. A questo punto, il percorso avrà un peso totale di 80 (40 x 2), decisamente sconveniente rispetto a quello di roccia (il cui peso rimane di 45).
È ovvio che un'intelligenza artificiale così avanzata deve essere adeguatamente supportata dalla grafica tridimensionale: la presenza di pioggia, e la relativa intensità, devono essere ben rappresentate; in caso contrario la scelta di un percorso più lungo potrebbe apparire quanto meno bizzarra.
In queste pagine abbiamo introdotto l'argomento pathfiding, la tecnica qui spiegata è alla base dell'intelligenza artificiale di un "giochino" come il primo Civilization (e anche in buona parte di Civilization 2); il mitico e sopraffino gioco di strategia che ha venduto milioni di copie in tutto il mondo.
Nel prossimo futuro ci torneremo, approfondendo tecniche più complesse e moderne e osserveremo esempi di codice sfruttato dai programmatori professionisti nella realizzazione dei best-seller che trovano spazio nei nostri hard disk.
Anche in questo caso, in fondo, è tutta una questione di... peso!



Caccia alla cella

Il cellulare ci spia? Noi spiamo lui. Come tenere sotto controllo i nostri spostamenti nella rete GSM

Durante una telefonata effettuata mentre siamo in movimento, in macchina o in treno, il nostro telefonino scambia continuamente informazioni con le antenne del nostro operatore telefonico a cui si aggancia e sgancia mentre cambiamo di posizione.
Il funzionamento delle reti cellulari, basato su questo comportamento, permette così al gestore di telefonia mobile di trovare con buona precisione l'utente in un punto qualsiasi del territorio coperto. Queste informazioni tecniche in teoria sono riservate solo agli addetti ai lavori, ma noi possiamo vederle tramite CellTrack, un software freeware che funziona sulla maggior parte degli smartphone con sistema operativo Symbian.
Il software va scaricato dal sito ufficiale del produttore (www.afischer-online.de/sos/celltrack) nella versione corretta per il proprio telefonino.



:: Conosciamo il programma

Una volta avviato il programma, ci troveremo nella finestra principale, denominata "Cell".
Vediamo cosa stiamo visualizzando:

- **Cellid**: è l'identificativo numerico della "cella" in cui ci troviamo in questo momento, ossia della specifica sottoarea all'interno della rete del gestore telefonico (in parentesi in formato esadecimale, hex).
- **LAC**: è il codice di localizzazione dell'area della cella in cui ci troviamo (tra parentesi in hex).
- **Net**: è il codice che identifica il gestore telefonico sul quale ci troviamo (es. 222 01 per TIM su GSM, 222 99 per 3 ITA) e viene visualizzato anche il tipo di rete GSM o WCDMA (comunemente chiamato UMTS).
- **Name**: qui viene visualizzato il nome dell'antenna; è però necessario che nei "Settings" abbiamo imposta-



to “Cell Name from Id” o “Cell Name from CBS”, se l’informazione viene effettivamente inviata dal gestore, su ON (per CBS, il canale di broadcast va impostato su 50 per l’Italia). In caso contrario verrà visualizzato solo un trattino.

- **Signal**: mostra la qualità del segnale in ricezione dall’antenna BTS (quello che viene mostrato con le “tacche” nei telefonini) in percentuale e come attenuazione in dBm.
- Sulla destra è mostrato un indicatore grafico del livello di batteria
- Nell’ultima riga in basso è mostrata una descrizione associata alla cella che il software pesca dal suo database e che possiamo modificare o impostare a nostro piacimento.
- Nel diagramma si vede l’andamento dinamico del segnale: in verde il valore dBm, mentre la linea nera corrisponde alla percentuale; in rosso sono visualizzati i cambi di cella.

:: Sempre più in dettaglio

Con i cursori che usiamo per spostarci nei menu del telefono possiamo passare alla seconda finestra del programma“Cell More”.
In quest’area troviamo ulteriori dettagli sulla cella cui siamo connessi.

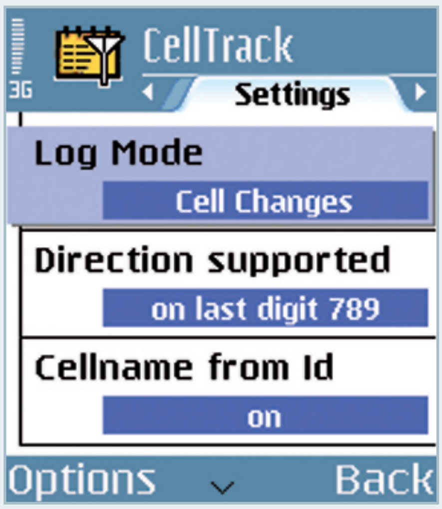


Nella terza finestra, “Cell Pic”, possiamo addirittura associare una foto alla cella. Per prima cosa dobbiamo salvare, o spostare, l’immagine nella cartella dove abbiamo installato CellTrack.
Il nome del file dovrà avere questo formato **CCCCLLLLCCCDD.jpg**, dove:

- **CCCC**=CellId (hex);
- **LLLL**=LAC (hex);
- **CCC**=identificativo nazione (222 per l’Italia);
- **DD**=identificativo provider (CCCDD corrisponde a Net).



Nella quarta finestra, “Phone”, vengono riportate alcune in formazioni sul nostro telefonino, tra cui la versione del sistema operativo installata.



Nella quinta finestra, “Log”, troviamo la cache di tutte le celle a cui ci siamo collegati anche se per soli pochi secondi, con relativo campo descrittivo nel caso l’avessimo inserito in precedenza.
Infine, nella sesta e ultima finestra, “Description”, possiamo inserire una descrizione arbitraria della cella in cui ci troviamo, informazione che poi apparirà nella finestra “Cell”.

QUALE SYMBIAN?

Se non si è sicuri di avere una determinata versione di Symbian consiglio di installare la release per la versione 6.2 che funziona sicuramente. Una volta lanciata sarà possibile leggere anche la versione esatta di Symbian che si possiede e sostituire eventualmente CellTrack con la versione opportuna.

symbian

:: Come funziona

Il funzionamento principale del software è quello di registrare i cambi di cella che avvengono durante il normale uso del telefono.
Sono presenti diverse modalità di registrazione che possiamo impostare nel menu Settings. Clicchiamo su Logging: qui possiamo cambiare la modalità di registrazione: nessuna (No Log), nuove celle incontrate (New Cells only), cambio di cella (Cell Changes), variazioni di segnale (Signal Changes), modalità manuale (Log manual), modalità server (Run as Server). Per una registrazione automatica, basta lasciare l’ultima (Run as Server). Con il log manuale viene registrata l’informazione solo quando viene premuto il tasto di selezione del telefonino.
Nei test effettuati non abbiamo riscontrato un supporto all’identificazione della cella (Cellname from Id) da parte dei gestori italiani. Se disponibile, questa informazione ci permette di avere ulteriori informazioni sulla direzione in cui ci stiamo spostando. Anche in questo caso sono presenti diverse tipologie di gestione selezionabili nel menu “Direction supported” e “Direction Digit Position”. Tutte le informazioni registrate vengono compresse in un database che può essere scambiato con altri utenti e in rete si possono trovare database già completati (ad es. per WIND) che è possibile importare nel proprio telefonino!

Massimiliano Brasile